Stubblebine 109755con-1

REMARKS

Claim 56 was rejected under 35 USC 102 as being anticipated by Abadi et al. Since the only citation that mentions Abadi et al is an article that which was published by the ACM, titled "A Semantics for a Logic Authentication," it is assumed that the rejection is based on this article. Applicant respectfully traverses the rejection.

Claim 56 defines a system with five means. The Examiner asserts that each of the "means" limitations is met by the Abadi et al reference as follows:

(1) means for preparing a revocation authority statement	Page 204, col. 1 and 2 (i.e., page 204, since it contains only 2 columns.
(2) means for preparing a freshness statement	ditto
(3) means for preparing a validity statement	ditto, and section 2.3 on page 205
(4) means for providing the above three statements to a revocation authority	Page 204 and 205
(5) means for selectively verifying	ditto

Applicant respectfully disagrees that the cited passages teach that which the Examiner asserts. The Abadi et al article is a language tutorial. In the introduction it presents a simple authentication protocol that is associated with an arrangement where principals A and B, who trust server S, engage server S to provide a key for encrypted communication between the principals. In the introduction (pages 201, 202, and a portion of page 203, Abadi et al also address the fact that an earlier article by Burrows et al (where Abadi is a co-author) invented a language for dealing with protocols in a formal manner, that the previous semantics of that language were confusing, that Abadi et al improved the created syntax and semantics, and that the remainder of the article is devoted to describing an improved syntax. Section 2 of the article (which covers pages 203, 204, the left column of page 205, and a portion of the right column of page 205) reviews the teachings of aforementioned Burrrows et al article.

Page 204 of the article is devoted, basically, to a presentation of a number inference rules. Each rule is presented in the form of an equation, followed by text that explains what the equation says. No means whatsoever are presented at page 204 of the article.

Stubblebine 109755con-1

Page 205 focuses on the syntax used to express the logic that the protocol processing entails. Here, too, no means whatsoever are presented.

Basically, the passages contained in the pages cited by the Examiner are totally abstract. They pertain to the teaching of a language; not to any particular system. Moreover, each of the teachings, though contributes to the theory, is quite disjoint from the other teachings. They are more like the collection of Newton's laws of motion, than a combination of elements that form a system.

nope - relate to freshness rule

In contradistinction, claim 56 defines a system that operates pursuant to a specific policy. The first element of claim 56 specifies a means "for preparing a statement" in response to the policy. The statement is "of an assigned revocation authority in a distributed system network in response to a policy, said revocation authority statement being associated with an initial statement." That is, the policy-driven statement specifies a means that creates a statement x, and that statement x specifies an "assigned revocation authority." Moreover, the statement that is created, according to the claim, is "associated with an initial statement." The reference teaches no "policy," teaches no statement pursuant to a policy, and teaches no "initial statement." Additionally, no actual means is described in page 204 of the Abadi et al article, and the Examiner has not pointed to any.

The second element of claim 56 specifies a means "for preparing a statement of a freshness constraint period," also in response to the policy, and this statement of freshness is associated with the same revocation authority. Admittedly, the notion of freshness is found in the Abadi et al reference, but no means is described in page 204 of the Abadi et al article (or elsewhere) that has the specific attributes defined in claim 56. It is noted that the Examiner has not pointed to any means either.

The third element of claim 56 specifies a means for "preparing a validity statement at said assigned revocation authority in the distributed system network." This statement is also prepared in response to the policy. The statement includes a verification status at some temporal reference. Admittedly, the notion of freshness carries with it the notion of time, but no means is described in page 204 of the Abadi et al article (or elsewhere) that describes a means (a computer, a device, an entity) that specifies a time and merely states that, at the specified time, the status is "OK," or "not OK."

Stubblebine 109755con-1

The fourth element of claim 56 specifies a means for communication. That is, a means for communicating to a verification authority the statements created in the first three means. The Examiner points to pages 204 and 205 generally but, as applicant reads the cited passages, no communication element (or any other concrete physical element) is described therein.

Lastly, the fifth element of claim 56 specifies a means, at the verification authority, for selectively verifying the initial statement relative to the statements created in the first three means. Again, applicant respectfully submits that pages 204 and 205 that were cited by the Examiner do not describe or suggest such means.

To conclude, in applicant's view, none of the elements of the system defined by claim 56 are found in the Abadi et al article, and certainly not in the pages cited by the Examiner. Therefore, applicant respectfully submits each of the claim's elements constitutes a separate reason to hold that claim 56 is not anticipated by Adabi et al and, of course, the combination of the claim's elements forms a compelling reason to hold that claim 56 is neither anticipated nor made obvious by Adabi et al.

Claims 52-54 were rejected under 35 USC 103 as being unpatentable over Abadi et al in view of Denning et al. Applicant respectfully traverses.

Since the only citation to anything that is by Denning et al, is an article that was published in *Communications of the ACM*, titled "Timestamps in Key Distribution Protocols," it is assumed that the Examiner's reference to Denning et al refers to this article.

With respect to claim 52, the Examiner asserts that the first paragraph in col. 2 of page 201 teaches "deriving freshness constraints from initial polity assumptions and an authentic statement." Applicant respectfully disagrees. The cited paragraph teaches that a server, in response to a request sends a message $\{T_s, K_{ab}\{T_s, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$. It is noted that no policy is mentioned, and no assumptions are made from a policy. Moreover, although this message has a time element, the cited paragraph does not extend this to a *freshness* notion. Time, per se, says nothing about freshness. To include the notion of freshness, one must consider another point in time for the purpose of comparing the initial time thereto, and making a determination as to whether the initial time is still "fresh." No such notion is presented in the cited paragraph. Certainly, there is no notion

of a "freshness constraint" that might specify, for example the duration during which time a message, or a statement, or a status, is considered "fresh." All that the paragraph states, relative to time, is that the message contains a timestamp and that "since the message contains a recent timestamp T_s, A believes that S sent the message recently." The term "recently" is certainly quite ambiguous.

Thus, in connection with the first step of claim 52, there is no policy in Abadi et al, there is no freshness constraints that are specified in Abadi et al, and there is certainly no deriving of freshness constraints from "initial policy assumptions and an authentic statement." In other words, in applicant's view Abadi et al do not teach the first step of claim 52. Since the Denning et al article is cited merely for its teachings of the exact equation found in step (c) of the claim 52 method, and not in connection with the first step of claim 52, it follows that the first step is not taught or suggested by the Abadi et al and Denning et al combination of references and that, consequently, claim 52 is not obvious in view of the Abadi et al and Denning et al combination of references.

The second step of claim 52 defines imposing "freshness constraints by employing recent-secure authentication principle to effect revocation." The Examiner again asserts that col. 2 of page 201 teaches this step. Respectfully, applicant disagrees. Since the substance of col. 2, of page 201 was already addressed above, for sake of brevity directs the Examiner's attention to the above remarks regarding what the first paragraph does, and does not teach about the subject of freshness. It is applicant's view that the cited paragraph does not teach the second step of claim 52 and that, therefore, claim 52 is not obvious in view of the Abadi et al and Denning et al references.

As for the third step of claim 52, the Examiner points to an equation in the Denning et al reference. Contrary to the Examiner's assertion, the equation in the Denning et al reference is **not**

$$\left|t_{now} - t_{timestamp}\right| \leq \delta. \qquad (1)$$

Rather, it is $|Clock - T| < \Delta t1 + \Delta t2$, where $\Delta t1$ is an interval representing the normal discrepancy between the server's clock and the local clock, and $\Delta t2$ is the interval representing the expected network delay time. Realizing that variables can be expressed

in different letters, applicant would agree that the Denning et al equation could be written as

$$\left|t_{now} - t_{timestamp}\right| \leq \Delta t1 + \Delta t2, \qquad (2)$$

making the left sides of equations (1) and (2) the same. However, the right sides are qualitatively different. That is, the right sides are not the same mathematically, and they are not the same conceptually. In equation (1), the right side is a single constant that is selected by an administrator. This single constant can be any value and is, therefore, relatively arbitrary. This single constant represents a measure of desired freshness, which represents the time range during which the administrator is willing to accept something (a "particular assertion") as *fresh enough*. In contradistinction, the right hand side of equation (2) is the sum of two elements that a grounded in the physical characteristics of a network. One of the elements ($\Delta t2$) represents the physical delay of the network and, therefore, it is a value that is not chosen, but dictated by the network. It does not represent a freshness notion but, rather, it MUST be included in order for anything to work -- since the network delay is unavoidable and must be accounted for. The second element ($\Delta t1$) represents the difference in clock values of two network nodes, and this element is even further removed from any notion of freshness notion. As long as the two network nodes are not synchronized with each other, this element MUST be includes in order for anything to work.

To conclude, it is applicant's view that although the two left sides of equations (1) and (2) are the same, the two right hand sides are completely different. Therefore, the third step of claim 52 is not obvious in view of the Abadi et al and the Denning et al references.

Since none of the three steps of claim 52 are suggested by these references, applicant believes that claim 52 is clearly patentable of these references.

As for claim 53, it is amended herein to make it clearer, and applicant believes that, like the unamended claim, amended claim 53 is not obvious in view of the references. Relative to the first clause of claim 1, which defines a means for creating a time-stamped validity assertion message, the Examiner points to the fifth sentence of page 202 in the Abadi et al reference, which states:

> Some of these concepts are illustrated in the protocol above: *good keys* are used to determine who has sent the various messages, a *trusted authority* (the server) is trusted to generated good encryption keys, and timestamps are used to prove that messages are *fresh*, meaning that they have not been sent before the start of the current authentication.

This sentence refers to the server sending "good encryption keys." Though it does not actually say that the server's message that contains the encryption keys contains a timestamp as well, the Abadi et al Figure 1 does show a timestamp, T_s. This time is used by the recipient principals to decide whether to accept the encryption keys, and in that sense, this timestamp does constitute a freshness measure. Hence, applicant agrees that the server's message can be characterized as a *time-stamped message*. However, it cannot be characterizes as a *time-stamped message that constitutes a "validity assertion message pertaining to the validity of an initial assertion,"* which is what claim 53 specifies, because it does not contain a "validity assertion message," and it contains no message whatsoever "pertaining to the validity of an initial assertion." Therefore, applicant respectfully submits that the first element of claim 53 is not suggested by the Abadi et al reference. Since the Denning reference is presented solely for its teachings of the equation (which is found in the third element of the claim), it follows that the first element of claim 53, and consequently the entirety of claim 53, is not obvious in view of the Abadi et al and Denning combination of references.

As for the second element of claim 53, which defines a means for asserting a freshness constraint -- separate and apart from the assertion message of the first element --, the Examiner asserts that lines 1-21 of Abadi et al's page 204 (col. 1) teaches this element. Applicant respectfully disagrees. Line 1 defines a message-meaning rule, and lines 2-10 explain the rule as:

> The first rule says that if P believe that P and Q share a key K and P sees a message encrypted with K (presumably known only to P and Q), then P believes that Q sent the message. However, P must e certain that it did not simply send the message o itself, and the side condition that $P \neq R$ reflects the assumption that a principal can detect and ignore its own message.

The explanation above says nothing about freshness, and by extension, the equation at the top of col. 1 of page 204 also says nothing about freshness.

Stubblebine 109755con-1

The second equation of the page, on line 12, is explained in lines 13-21 as follows:

> [the equation] says that if P believes a message is fresh and that Q sent the message, then P believes that Q sent the message recently, and still believes the contents of the message. The name "nonce-verification" comes from the fact that the freshness of X is typically proven by including a nonce in the message X. A nonce is an expression (such as a timestamp) invented for the purpose of being fresh, and included in the messages to prove their freshness.

This passage does mention freshness, but it does not teach any explicit constraint in the message, other than the message being "recent." In contradistinction, the second step of claim 53 specifies a "a length of time... relating to said initial assertion." Since no length of time is specified in the passage cited by the Examiner or elsewhere in the Abadi et al reference, applicant respectfully submits that the second step of claim 53 is not suggested by the Abadi et al and Denning et al references and that, therefore, claim 53 is not obvious in view of the Abadi et al and Denning et al references.

As for the third step of claim 53, which contains the same equation that is found in claim 52, applicant respectfully submits that the Denning et al do not teach the limitations of this step. For sake of brevity, the Examiner is respectfully directed to the remarks above, regarding claim 52.

Since none of the steps defined in claim 53 are suggested by the Abadi et al and the Denning et al references, applicant respectfully submits that claim 53 is not obvious in view of the Abadi et al and Denning et al references.

As for claim 54, it defines a method for protecting the authority of a "distinguished principal" -- which is an authenticating authority. The closest that the Abadi et al reference comes to an authenticating authority is the server S that provides the keys. Therefore, the correspondence that the Examiner must establish relative to the Abadi el al reference is an assertion that the reference teaches a method for protecting the authority of the server S.

Regarding the first three means defined in claim 54, the Examiner asserts that Abadi et al teach these means at page 201, col. 2. Applicant respectfully disagrees. Applicant accepts that the first "means" of claim 54 (which for sake of clarity is defined in amended claim 54 as "first means") is taught, because Figure 1 shows the server S.

However, nothing is described to correspond to the second "means" of claim 54 (which for sake of clarity is defined in amended claim 54 as "second means"), and nothing is described to correspond to the third "means" of claim 54 (which for sake of clarity is defined in amended claim 54 as "third means"). Therefore, applicant respectfully submits that claim 54 is not obvious in view of the Abadi et al reference; and since the Denning et al reference is not presented for any teachings relative to the first three means of claim 54, it follows that claim 54 is not obvious in view of the Abadi et al and the Denning et al reference.

As for the fourth means of claim 54, applicant respectfully directs the Examiner's attention to the above remarks regarding a similar means in claim 53.

Claim 55 was rejected under 35 USC 103 as being unpatentable over Van Oorschot et al, US Patent 5,699,431 in view of Denning et al. Applicant respectfully traverses.

Claim 55 specifies a system for issuing certificates, which is defined to comprise means for issuing certificates, means for asserting (specifying) a principal, means for delegating, and means for asserting (specifying) freshness constraints. According to the Examiner these four means are taught by Van Oorschot et al in col. 1, lines 30 through col. 2, line 9. The claim also defines a means for verifying, and according to the Examiner, this means is taught by Denning et al. Applicant respectfully traverses.

The passage cited in the Van Oorschotet al patent does not teach any means. It is simply a discussion of the fact that public keys are distributed by public key certificates, and that such certificates have certain attributes. The discussion also covers the notion of a natural expiration date of certificates, and that if -- for some reason -- it is desired to revoke an unexpired certificate, one can consult a certificate revocation list (CRL).

One might assume that some means exist for creating and sending out such public key certificates, even though the text does not explicitly mention such means. More specifically, a certification authority (CA) is mentioned and one might assume that the CA has a means for creating the certificates. One might also assume that the CRL is stored in some means, even though the text does not explicitly mention such means. However, it is respectfully submitted that the Examiner's assertion of means that are taught by Van Oorschot et al is based solely on what is assumed to exist; not on actual

teachings. More importantly, a careful scrutiny of the defined claim elements reveals that those elements have limitations that are not necessarily required for the Van Oorschot et al system to operate and, therefore, cannot be assumed to exist.

The first means defined in claim 55 specifies a "means for issuing certificates for principals within an organization by the organization" (emphasis supplied). In contradistinction, the reference teaches that the public key certificate is issued NOT by the organization, or person, who needs the public key, but by "a trusted third party (commonly called the certification authority or CA)." In other words, the reference teaches away from claim 55.

The second means defined in claim 55 specifies a "means for asserting, by the organization, a principal authorized as an authority for issuing time stamped certificates." The interpretation that corresponds best to the Examiner's assertion is that the certificates issued by the CA are time stamped and that the CA constitutes the "authority for issuing time stamped certificates." Of course, that forces the first means and the second means to both correspond to the CA -- or at least to different portions of the CA.

The third means defined in claim 55 specifies a "means for delegating authority for issuing time stamped certificates." This specifies some means that "delegates authority." No such means is described or suggested in the Van Oorschot et al reference. There is simply no discussion as to how an entity that seeks a certificate knows the identity of the CA, and certainly there is no notion of something "delegating" authority.

The fourth means defined in claim 55 specifies a "means for asserting freshness constraints on assertions." Applicant respectfully submits that a revocation list is NOT a freshness constraint, unless the Examiner is to assert that the fact that "the serial number of the certificate in question does not appear on the most recent valid CRL" (col. 2, lines 8-9) is indicative of freshness.

Lastly, the fifth means defined in claim 55 specifies a "means for verifying that a relation $\left|t_{now} - t_{time\ stamp}\right| \leq \delta$ is satisfied for each particular assertion necessary for verification of a secure channel, where $t_{time\ stamp}$ being a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary

freshness constraint pertaining to the particular assertion and t_{now} being the time of verification." To the extent that the Examiner might assert that the CRL does constitute a freshness constraint assertion, it is quite clear that a revocation contain in the CRL does not contain a time. The mere fact that "the serial number of the certificate in question does not appear on the most recent valid CRL" clearly obviates the need for including a time in the CRL.

Regarding the equation that is embedded in the defined fifth means, the Examiner asserts that Denning et al teach this equation. Even if that were the case, the Van Oorschot et al reference does not NEED a time indication in the CRL and, therefore, there is nothing to be gained by the Denning et al teachings. In any event, as demonstrated above in connection with claim 52, Denning et al do not teach the equation embedded in the fifth means of claim 55.

In short, applicant respectfully submits that claim 55 is not obvious in view of Van Oorschot et al in combination with Denning et al.

In light of the above amendments and remarks, applicant respectfully submits that all of the Examiner's rejections have been overcome. Reconsideration and allowance of the outstanding claims are respectfully solicited.

Respectfully,
Stuart Gerald Stubblebine

Dated: 3/27/04

By _____
Henry T. Brendzel
Reg. No. 26,844
Phone (973) 467-2025
Fax (973) 467-6589
email brendzel@comcast.net